デジタル社会を支える数学

数理科学研究科　教授　桂　利行

現在はデジタル機器の時代である . コンピュータ、CD、CD-ROM、カメラ、ビデオ、電話、ビデオカセットデッキ、テレビに至るまで、デジタルが用いられるようになっている。 そのようなデジタル機器に欠かせない数学がある。それが**符号理論**である。デジタル信号に起こりがちな小さな誤りを訂正するこの理論によってデジタル機器の安定した作動が保証される。

かつてボイジャー 2 号が木星の写真をとり、その映像を地球に送って来たことがある。その美しさが世界中を魅了した。写真はデジタル信号にかえて地球に送られた。その信号が通信経路の途中で何の障害もなく地球にとどけば、正確な写真が再現される。しかし、宇宙線などによって信号が途中で変化し、地球で受信された信号がもとのものとは違っている可能性も存在する。したがって、正確な写真を再現するためには受信された信号から正しい情報をよみとるシステムが必要になる。このとき用いられるのが**誤り訂正符号**である。

状況を簡単にしてもう少し具体的な例をあげよう。信号は、数字 0 と 1 からなるとする。送信したい 1 つの信号が (0,1,0) であるとき、同じ数字を 3 個ずつ重ねて送ることにする。つまり、この例ではこの信号を (0,0,0,1,1,1,0,0,0) として送信する。このように無駄な情報を追加しておけば、どこか 1 箇所でエラーが生じても、多数決でもとの信号が再現できるわけである。たとえば (0,1,0,1,1,1,0,0,0) なる信号を受信した場合、もとの信号は (0,0,0,1,1,1,0,0,0) であったことが高い確率で推測されるであろう。

このように、余分な情報を付け加えることによって誤りをチェックするという考え方は身近なところでも用いられている。たとえば受験番号で 1A,2B,3C,4F,･･･ というような番号付けが用いられるが、この表示において A,B,C などは余分な情報である。しかし、たとえば 3C を過って 4C と入力したとすれば、そのような番号は存在しないから入力ミスをチェックすることができる。このように誤りをチェックするシステムを**誤り検出符号**という。写真を送る上記のような場合には、誤りを検出するだけではなく、誤りを訂正することが必要になる。この公開講座では符号理論がどのように構成され、誤り訂正がどのような原理で行われるかについてお話をしたい。

1. 符号理論の歴史

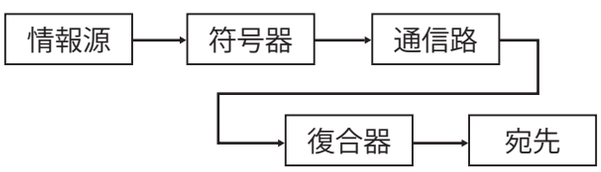
符号理論は 1948 年のシャノンの論文に始まるといえよう。彼は、ある条件が充たされれば符号長を大きくするに従い、誤り確率がいくらでも小さくなるような符号の列が存在することを示した。1950 年にはハミング符号が構成された。この符号はコンピュータの記憶装置の誤り訂正にしばしば利用される。1957 年には巡回符号が構成され、1959 年には BCH 符号が、1960 年には RS 符号が構成された。これらの符号は符号理論の中で重要な位置をしめる符号で

裏に続く

あり、RS 符号は BCH 符号の、BCH 符号は巡回符号の特殊なものである。また、RS 符号は CD や CD-ROM の誤り訂正符号として利用されている。1968 年にはバーレカンプ・マッシィ法という BCH 符号の効率的な復号法が考案されている。1971 年にはゴッパによりゴッパ符号が考案された。これは 1981 年にゴッパによって代数幾何符号として一般化された。1982 年には代数幾何符号を用いてそれまでは最良と思われていたバルシャモフ・ギルバート限界式を越える符号の列が構成され、代数幾何符号の理論的な優秀性が示された。1993 年にはフェン・ラオにより代数幾何符号の効率的な復号法が考案されるに至っている。

2. 符号とは ≥

情報源からの情報を符号化して送信し、受信する手続きを図式化すると次のようになる。



$\mathbf{F}_2$={0,1} とおく。n を自然数として

$$\mathbf{F}_2^n=\{x=(x_1,x_2,\cdots,x_n) \mid x_i \in \mathbf{F}_2(i=1,2,\cdots,n)\}$$

とおく。$\mathbf{F}_2^n$ の元 $(x_1,x_2,\cdots,x_n)$ を**語**あるいは**アルファベット**とよぶ。$\mathbf{F}_2^n$ の部分集合 C を**符号** (code) といい、n を C の**符号長**という。C の元を情報のアルファベットとして用い、冗長部分 $\mathbf{F}_2^n \setminus C$ を誤り訂正に用いる。

エラーを調べるために、$\mathbf{F}_2^n \ni x=(x_1,\cdots,x_n)$, $y=(y_1,\cdots,y_n)$ の距離を次のように定義する。

定義　ハミング距離

$$d(x,y)=\#\{1\leq i\leq n \mid x_i \neq y_i\}$$

ここに、集合 S に対して $\#S$ は S の元の数を表す。

この距離は次の 3 つの性質を満たす。

(i) $d(x,y)\geq 0$. また、$d(x,y)=0 \longleftrightarrow x=y$.

(ii) $d(x,y)=d(y,x)$

(iii)[三角不等式] $d(x,y)+d(y,z)\geq d(x,z)$

定義 $\mathbf{F}_2^n$ の部分集合 C に対し、その**最小距離** d を次のように定義する：

$$d=\min\{d(x,y) \mid x,y \in C, x \neq y\}$$

ここに、min は最小値を表す。

定義符号 C（$\subset \mathbf{F}_2^n$）の元の数が k でその最小距離が d のとき、C を (n,k,d)- **符号**という。

符号 C の重要な量は、符号長 n、元の数 k、最小距離 d の 3 つの量である。それらが決まれば符号 C の性質は確定する。

3. 参考文献

[1] 岡本和夫著「社会と自然を貫く数学」第 12 章（放送大学教材、2007）

[2] 桂利行著「デジタルの数学」（「数学のたのしみ」21 号、2000 年 10 月、54--65、日本評論社。）

[3] 藤原良・神保雅一共著「符号と暗号の数理」（共立出版、1993。）

東京大学大学院理学系研究科・理学部
THE UNIVERSITY OF TOKYO SCHOOL OF SCIENCE
〒 113-0033　東京都文京区本郷 7-3-1
03（5841）7585